IN THE CLAIMS

Please amend the claims as follows:

1. (Currently amended) A computer device having wireless communication capability, comprising:

a wireless communication portal for selectively sending and receiving data across a wireless network;

a computer platform including a resident application environment configured to selectively download applications to the computer platform ~~through the portal~~, the resident application environment configured to selectively download applications through the portal that comply with a predefined security protocol;

a data store in communication with the computer platform and selectively sending data to and receiving data from the computer platform; and

a download manager resident on the computer platform that is configured to selectively download applications through the portal that do not comply with the predefined security protocol,

wherein the selectively downloaded applications that comply with the predefined security protocol are executed by the computer platform within the resident application environment, and

wherein the selectively downloaded applications that do not comply with the predefined security protocol are executed by the download manager outside of the resident application environment.

2. (Original) The device of claim 1, wherein the download manager exists within resident application environment and uses an existing application download interface.

3. (Currently amended) The device of claim 1, wherein [[the]] a downloaded application that does not comply with the predefined security protocol is immediately executed.

4. (Original) The device of claim 1, wherein a downloaded application that does not comply with the predefined security protocol is stored, and the stored application is executed through the download manager.

5. (Canceled)

6. (Previously presented) The device of claim 1, wherein the download manager further manages storage of the selectively downloaded applications that do not comply with the predefined security protocol in the data store.

7. (Previously presented) The device of claim 1, wherein the predefined security protocol is verifying the origination of a given application to be downloaded.

8. (Previously presented) The device of claim 1, wherein the predefined security protocol is verifying the presence of a certificate within a given application to be downloaded.

9. (Canceled)

10. (Currently amended) A computer device having wireless communication capability, comprising:

a wireless communication means for selectively sending and receiving data across a wireless network;

a computer means selectively downloading applications ~~through the wireless communication means~~, the computer means configured to selectively download applications through the wireless communication means that comply with a predefined security protocol; and

a means for selectively downloading applications through the wireless communication means that do not comply with the predefined security protocol,

wherein the selectively downloaded applications that comply with the predefined security protocol are executed by the computer means within the resident application environment, and

wherein the selectively downloaded applications that do not comply with the predefined security protocol are executed by the means for selectively downloading applications outside of the resident application environment.

11. (Previously presented) A method of selectively downloading through a wireless connection to a computer device, comprising the steps of:

downloading, from the wireless connection to the computer platform of the computer device, an application that does not comply with a predefined security protocol for use at that computer device, the computer platform including a resident application environment for downloading applications utilizing a predefined security protocol and for executing applications downloaded in compliance with the predefined security protocol within the resident application

environment, the downloading of the non-complying application occurring through the use of a download manager resident on the computer platform; and

executing the non-complying application at the computer device with the download manager outside of the resident application environment.

12. (Original) The method of claim 11, wherein the download manager exists within resident application environment and the step of downloading uses an existing application download interface.

13. (Previously presented) The method of claim 11, further comprising the steps of:

storing, with the download manager, the non-complying application; and

executing the stored application through the download manager.

14. (Previously presented) The method of claim 11, further comprising the step of verifying whether the non-complying application complies with the predefined security protocol.

15. (Previously presented) The method of claim 14, wherein the step of verifying includes verifying the presence or absence of a certificate within the non-complying application.

16. (Canceled)

17. (Previously presented) The method of claim 11, further comprising the step of downloading the download manager to the computer platform of the computer device after a

request to download the non-complying application has been made, and prior to the step of downloading the non-complying application.

18. (Previously presented) A method of selectively downloading through a wireless connection to a computer device, comprising the steps of:

a step for downloading, through the wireless connection to the computer platform of the computer device, an application that does not comply with a predefined security protocol for use within a resident application environment at that computer device; and

a step for executing the downloaded application at the computer device outside of the resident application environment,

wherein applications that comply with the predefined security protocol are configured for execution within the resident application environment.

19. (Previously presented) A non-transitory computer-readable medium containing program code stored thereon, that when executed by a wireless computer device causes the device to perform the steps of:

downloading through a wireless connection to a computer platform of the computer device an application that does not comply with a predefined security protocol for use at that computer device, the computer platform including a resident application environment for downloading applications utilizing a predefined security protocol and for executing applications downloaded in compliance with the predefined security protocol within the resident application environment, the downloading of the non-complying application occurring through the use of a download manager on the computer platform; and

executing the non-complying application at the computer device with the download manager.

20. (Previously presented) The non-transitory computer-readable medium of claim 19, wherein the download manager is resident on the computer platform.

21. (Previously presented) The non-transitory computer-readable medium of claim 19, wherein the download manager is loaded to the computer platform after a request to download of the non-complying application and prior to download thereof.

22. (Previously presented) The computer device of claim 1,

wherein the download manager exists within resident application environment and uses an existing application download interface.

23. (Previously presented) The computer device of claim 1, wherein the predefined security protocol includes an application validation requirement of the resident application environment.

24. (Previously presented) The computer device of claim 1, wherein the applications being downloaded by the resident application environment in compliance with the predefined security protocol and the applications being downloaded by the download manager in non-compliance with the predefined security protocol are both stored in the data store.

25. (Previously presented) The computer device of claim 1, wherein the predefined security protocol is configured to protect the computer device.

26. (New) The computer device of claim 1, wherein compliance with the predefined security protocol for a given application is based upon information contained with the given application during download and prior to execution of the given application.

27. (New) The computer device of claim 1,

wherein the resident application environment is requested to download a given application,

wherein the resident application environment refuses to download the given application based on the given application failing to comply with the predefined security protocol,

wherein the download manager is subsequently requested to download the given application after the refusal, and

wherein the download manager downloads the given application responsive to the subsequent request.